Express Mail Label No. EL543500064US

10-19-00

4

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
2204/A61

Total Pages in this Submission
32

TO THE ASSISTANT COMMISSIONER FOR PATENTS
Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

LOCAL FIREWALL APPARATUS AND METHOD

and invented by:

Stephen S. Jackson

If a CONTINUATION APPLICATION, *check appropriate box and supply the requisite information:*

❏ **Continuation**　❏ **Divisional**　❏ **Continuation-in-part (CIP)**　of prior application No.: _____

Which is a:

❏ **Continuation**　❏ **Divisional**　❏ **Continuation-in-part (CIP)**　of prior application No.: _____

Which is a:

❏ **Continuation**　❏ **Divisional**　❏ **Continuation-in-part (CIP)**　of prior application No.: _____

Enclosed are:

Application Elements

1. ❏ Filing fee as calculated and transmitted as described below

2. ☒ Specification having _____20_____ pages and including the following:

    a. ☒ Descriptive Title of the Invention

    b. ❏ Cross References to Related Applications *(if applicable)*

    c. ❏ Statement Regarding Federally-sponsored Research/Development *(if applicable)*

    d. ❏ Reference to Microfiche Appendix *(if applicable)*

    e. ☒ Background of the Invention

    f. ☒ Brief Summary of the Invention

    g. ☒ Brief Description of the Drawings *(if drawings filed)*

    h. ☒ Detailed Description

    i. ☒ Claim(s) as Classified Below

    j. ☒ Abstract of the Disclosure

P01ULRG/REV04

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No. 2204/A61
Total Pages in this Submission 32

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*

     a. ☐ Formal   Number of Sheets _____

     b. ☒ Informal   Number of Sheets   4

4. ☒ Oath or Declaration

     a. ☐ Newly executed *(original or copy)*   ☒ Unexecuted

     b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*

     c. ☒ With Power of Attorney   ☐ Without Power of Attorney

     d. ☐ *DELETION OF INVENTOR(S)*
        Signed statement attached deleting inventor(s) named in the prior application,
        see 37 C.F.R. 1.63(d)(2) and 1.33(b).

5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
    The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.

6. ☐ Computer Program in Microfiche *(Appendix)*

7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*

     a. ☐ Paper Copy

     b. ☐ Computer Readable Copy *(identical to computer copy)*

     c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☐ Assignment Papers *(cover sheet & document(s))*

9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*

10. ☐ English Translation Document *(if applicable)*

11. ☐ Information Disclosure Statement/PTO-1449   ☐ Copies of IDS Citations

12. ☐ Preliminary Amendment

13. ☒ Acknowledgment postcard

14. ☒ Certificate of Mailing

     ☐ First Class   ☒ Express Mail *(Specify Label No.):* EL543500064US

P01ULRG/REV04

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)
(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
2204/A61

Total Pages in this Submission
32

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
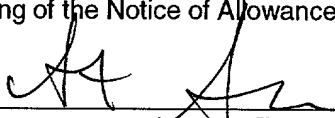
16. ☐ Additional Enclosures *(please identify below):*

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate		Fee
Total Claims	29	- 20 =	9	x	$18.00	$162.00
Indep. Claims	5	- 3 =	2	x	$80.00	$160.00
Multiple Dependent Claims (check if applicable) ☐						$0.00
					BASIC FEE	$710.00
OTHER FEE *(specify purpose)*						$0.00
					TOTAL FILING FEE	$1,032.00

☐ A check in the amount of _____ to cover the filing fee is enclosed.

☐ The Commissioner is hereby authorized to charge and credit Deposit Account No. _____ as described below. A duplicate copy of this sheet is enclosed.

    ☐ Charge the amount of _____ as filing fee.

    ☐ Credit any overpayment.

    ☐ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.

    ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

_____
Signature

Steven G. Saunders, Reg. No. 36,265
BROMBERG & SUNSTEIN LLP
125 Summer Street
Boston, MA 02110
(617) 443-9292

Dated: October 18, 2000

cc:

P01ULRG/REV04

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)	Docket No.
Applicant(s): Jackson	2204/A61

Serial No. Not Yet Assigned	Filing Date Herewith	Examiner Not Yet Assigned	Group Art Unit Not Yet Assigned

Invention: LOCAL FIREWALL APPARATUS AND METHOD

I hereby certify that this ___Utility Patent Application Transmittal and enclosures referred to therein___
(Identify type of correspondence)

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under

37 CFR 1.10 in an envelope addressed to: The ~~Assistant~~ Commissioner for Patents, Washington, D.C. 20231 on
___October 18, 2000___
(Date)

___Steven G. Saunders___
(Typed or Printed Name of Person Mailing Correspondence)

___(Signature of Person Mailing Correspondence)___

___EL543500064US___
("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

P06A/REV02

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR UNITED STATES PATENT

FOR

LOCAL FIREWALL APPARATUS AND METHOD

Inventor:

Stephen S. Jackson
104 Antler Point Rd
Chapel Hill, NC 27516

Attorney Docket: 2204/A61
(12304RN)

Attorneys:

BROMBERG & SUNSTEIN LLP
125 Summer Street
Boston, MA 02110
(617) 443-9292

LOCAL FIREWALL APPARATUS AND METHOD

FIELD OF THE INVENTION

The invention generally relates to computer network security and, more
5   particularly, the invention relates to securing computer networks and computer
systems with firewalls.

BACKGROUND OF THE INVENTION

Local area networks (*e.g.*, intranets and other local networks) commonly
10   require some level of security to prevent data access by unauthorized people.
Such unauthorized people often are referred to as "hackers." Absent some
security measure, a hacker can access a local area network without permission by
the administrator of the network. For example, a hacker can illicitly copy secret
data from such a network, or reconfigure such a network to malfunction.

15   Various security measures often are taken to prevent access by a hacker.
Among those measures is use of a "firewall." As known in the art, a firewall is a
hardware and/or software device that controls access to a given network. For
example, a firewall may intercept all data received from a larger network (*e.g.*,
the Internet), and determine which data can pass through it to the network that it
20   is protecting. Data access can be permitted based upon a variety of
preconfigured policies, such as the type of transport protocol used by received
data, or the origin of the data. A firewall thus acts as a filter to prevent
unauthorized data from being transmitted to and/or being removed from its
protected network.

25   Although useful in many instances, the security provided by a firewall can
be breached. In such case, all computer systems in such protected networks
consequently can be susceptible to being accessed and/or tampered with by a
hacker.

SUMMARY OF THE INVENTION

In accordance with one aspect of the invention, a firewall that may be used in a power integrated network having a plurality of computer systems is powered by the power integrated network. To that end, the firewall includes an input module that receives data addressed to a given computer system in the power integrated network, a security module for determining if the data received at the input module can be forwarded to the given computer system, and a power module to power both the input module and the security module. The power module receives its power from the power integrated network.

In various embodiments, the power integrated network implements principles of Power Ethernet. Moreover, the power module may include a power converter that converts power received from the power integrated network into a power level that can be used by the security module and the input module. The firewall also may include an output module for forwarding the data to the given computer system. Of course, only data approved by the security module is forwarded to the given computer by the output module. The firewall further may include a policy server interface for communicating policy data with a policy server. The power integrated network generally includes at least two computer systems that are coupled with a cable that transmits both data and power.

In accordance with another aspect of the invention, a computer cable for communicating a first computer system with a second computer system in a power integrated network includes a firewall. In addition, the computer cable includes a data channel for transmitting data between the first computer system and the second computer system, and a power channel for transmitting power between the first computer system and the second computer system. The

firewall is coupled with both the data channel and the power channel and thus, is energized by the power received from the power channel.

The data channel may include one or more wires. In a similar manner, the power channel may include one or more wires. The computer cable may include a first coupler for coupling one end of the computer cable to the first computer system, and a second coupler for coupling a second end of the computer cable to the second computer system. A containment layer (*e.g.,* plastic) may circumscribe the data channel, firewall, and power channel.

In accordance with yet another aspect of the invention, a firewall for use in a self powering network may include program code for receiving data addressed to a given computer system in the network, program code for analyzing the received data to determine if the data can be forwarded to the given computer system, and a processor for executing the aforementioned program code. The processor is energized by the power integrated network.

In accordance with other aspects of the invention, a power integrated network coupled with a specified network includes a plurality of computer systems, a network firewall coupled between it and the specified network, and a local firewall coupled to one of the computer systems. The local firewall is powered by the power integrated network and prevents unauthorized access to the one computer system via the specified network. The local firewall prevents unauthorized access, however, to the one computer only.

Various embodiments of the power integrated network implement principles of Power Ethernet. In addition, the specified network may be a public network, such as the Internet.

In still other aspects of the invention, a method of securing a given computer system within a power integrated network receives power from the network, couples a local firewall to the given computer system, and uses the

received power to energize the local firewall. The local firewall is configured to control access to the given computer system.

BRIEF DESCRIPTION OF THE DRAWINGS

5   The foregoing and advantages of the invention will be appreciated more fully from the following further description thereof with reference to the accompanying drawings wherein:

      Figure 1 schematically shows a network arrangement that may be used with illustrative embodiments of the invention.

10   Figure 2 schematically shows an illustrative integrated network cable that may have an internal firewall configured in accord with illustrative embodiments of the invention.

      Figure 3 schematically shows the firewall shown in figures 1 and 2 in accordance with illustrative embodiments of the invention.

15   Figure 4 shows a portion of an illustrative process of initializing the firewall shown in figures 1-3.

DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

      In illustrative embodiments of the invention, a power integrated, local

20   network (*e.g.*, a local area network implementing Power Ethernet, discussed below) includes at least one computer system that has a local firewall in addition to, or instead of, a network firewall that protects the entire local network. The local firewall is energized by power received from the network. Details are discussed below.

25   Before continuing, the term "power integrated network" should be defined. Namely, the term "power integrated network" refers to a local network that transmits both power and data to member computer systems in the network. Such power may or may not be used by the member computer systems. Among

other ways, the power and data may be transmitted on a single cable via different wires, or via the same wire. Illustrative power integrated networks include Power Ethernet networks, which implement the proposed IEEE 802.3af standard. Currently, this standard is in draft form and is expected to be

5 completed and adopted sometime in late 2001. Computer systems utilizing this standard are capable of receiving power (*e.g.*, about fourteen watts) and data from a computer cable across an IEEE DTE (data terminal equipment) through a MDI (media dependent interface) compliant port. It should be noted, however, that although Power Ethernet and this IEEE standard are discussed, various

10 embodiments are not limited to such standard. Accordingly, various embodiments can be used on other types of networks that transmit both power and data.

It also should be noted that the term "data" is used herein to broadly represent any type of information that may be electronically transmitted across a

15 network. Such information may include, among other things, information commonly referred to as audio, video, signaling, control, and data. In addition, instead of using the term "datum," the term "data" is used herein to represent both the singular and plural form of the term "datum."

Figure 1 schematically shows an illustrative power integrated network 10

20 (hereinafter "network 10") coupled with a public network 12 (*e.g.*, the Internet). The network 10 includes a network firewall 14 to control the flow of network traffic into and out of the network 10, a central router 16, and a plurality of coupled computer systems 18. The computer systems 18 may be any computer device, such as network appliances, personal computers, or servers. Various

25 computer systems 18 each are coupled with a local firewall 20 that controls data traffic flow into and out of such computer systems 18. In the network 10 shown, one computer system 18 is not coupled with a local firewall 20, while three other computer systems 18 are coupled with a local firewall 20. Of course, in some

embodiments, any number of computer systems 18 may be coupled with a local firewall 20.

The network 10 also includes a policy server 22 that cooperates with the local firewalls 20 and/or the network firewall 14 to respectively protect against
5   unauthorized access into the computer systems 18 and network 10. In illustrative embodiments, the policy server 22 executes as a common open policy server ("COPS"). Of course, although desirable to use one, the network firewall 14 is not necessary. Accordingly, alternative embodiments do not include the network firewall 14.

10   Each computer system 18 having a local firewall 20 preferably is electrically coupled with the router 16 via a computer cable having an integrated local firewall 20. Such computer cable may plug into a wall jack having an Ethernet plug that is connected to the router 16. Figure 2 schematically shows such an illustrative computer cable 24. Specifically, the computer cable 24
15   includes a first connector 26 to couple with the computer system 18 (*i.e.*, with the IEEE DTE power by MDI interface), a local firewall 20, and a second connector 28 to couple with the router 16 (*e.g.*, via the above noted Ethernet plug). In illustrative embodiments, the computer system 18 being protected is in the same room as the wall jack. Accordingly, the firewall physically is located between
20   such computer system 18 and the wall jack within the same room. In such case, when servicing is necessary, the firewall 20 may be physically unplugged in the same room as the computer system 18.

The computer cable 24 further includes a plurality of wires 30 that respectively carry data and power channels between the two connectors 26 and
25   28. In illustrative embodiments, the wires 30 are used in conformance with the Power Ethernet standard. For example, both power and data may be carried by a single wire, or carried separately by separate wires. The local firewall 20 thus is coupled with the power channel to derive its power, and to the data channel to

both control data flow to and from its computer system 18, and to communicate with other devices in the network 10 (*e.g.*, the policy server 22). The computer cable 24 also includes an outer jacket made of some flexible insulating material, such as PVC plastic or rubber. Of course, the outer jacket may be any material

5   commonly used in the art to wrap around electrical wires.

In some embodiments, the local firewall 20 is not integrated into the computer cable 24. For example, the local firewall 20 may be directly coupled with a port on its protected computer system 18, or even within its protected computer system 18. When inside, the local firewall 20 may be a computer card

10   with the attendant functionality and/or a software module that, when executing, performs the desired functions. For example, the local firewall 20 may be implemented on the network interface card (not shown) of the protected computer system 18. In such case, the local firewall 20 is powered from the power integrated network 10 and not by the computer system 18. This permits

15   the firewall to be used to remotely query the computer system 18 to determine various information, such as whether the computer system 18 is then currently powered.

In still other embodiments, the local firewall 20 may be coupled with the Ethernet plug and thus, couple with its computer system 18 via a conventional

20   computer cable. For example, the local firewall 20 may be a separate box that plugs into the Ethernet plug and a standard cable that connects the computer system 18 with the Ethernet plug. Variants of such embodiments also may be integrated directly into the Ethernet plug. Many embodiments of the invention, however, include a local firewall 20 between one member computer system 18

25   and such computer system's connection to the local network 10.

Figure 3 schematically shows an illustrative local firewall 20 configured in accordance with illustrative embodiments of the invention. Among other things, the local firewall 20 includes an administration module 32 for ascertaining and

maintaining firewall configuration data, and a security module 34 for controlling computer access based upon the configuration data maintained by the administration module 32. In illustrative embodiments, both the administration module 32 and security module 34 are software components executing on a

5   microprocessor. Accordingly, the security module 34 may be firewall code (*e.g.*, based on SHASTA firewall code, from Nortel Networks Limited of Brampton, Ontario) that controls data flow to/from the computer system 18.

        To energize its components, the local firewall 20 includes a power module 36 for converting received power from the power integrated network 10. Since

10   illustrative embodiments receive a constant DC power supply, the power module 36 preferably is a simple DC power circuit that adjusts the power to an appropriate level for the local firewall 20. For example, such circuit may be an up-converter or a down-converter (*i.e.*, a buck converter). In alternative embodiments, the power converter can be configured in a more complex manner

15   to include conventional rectification and other circuitry for converting an AC power signal.

        The local firewall 20 also includes an interface 38 to communicate with other network devices (*e.g.*, the router 16, the policy server 22, and the attached computer system 18), and configuration memory 40 for storing configuration

20   data. Although only one is schematically shown, the interface 38 may be one single interface, or multiple interfaces. When data is received, the interface 38 forwards such data to the security module 34 for processing. The data then is forwarded to the computer system 18, via the interface 38, if the security module 34 determines that such data can be forwarded. Conversely, if the data is not

25   permitted to pass to the computer system 18, then the security module 34 may forward a message to a network administrator (*e.g.*, a server or other computer system 18) indicating that data has been rejected. The network administrator (which may be an actual person or automated software program) then may take

appropriate action, such as disconnecting the network device requesting access. In other embodiments, the security module 34 may be preprogrammed to take some other action.

The local firewall 20 preferably executes program code by means of a relatively low power, high performance microprocessor. In illustrative embodiments, a CRUSO™ microprocessor using an operating system based upon the VXWORKS™ operating system is used for such purposes. The CRUSO™ microprocessor is distributed by Transmeta Corporation of Santa Clara, California. The VXWORKS™ operating system is distributed by Wind River Systems, Inc. of Alameda, California. Of course, use of these elements is not necessary since other processors and operating systems may be used. Discussion of these elements thus are for illustrative purposes only.

A tamper module 42 also may be included in the local firewall 20 to monitor power flow to the local firewall 20. Details of the tamper module 42 are discussed below. Other components not shown in the figures also may be included in the local firewall 20. For example, the local firewall 20 may include the IP stack, multicast functionality, a Java Virtual Machine ("JVM"), and other memory. Among other reasons, multicast functionality may be included to permit the local firewall 20 to be remotely controlled and/or configured. Those skilled in the art should understand that the local firewall 20 may include these and other elements for its use.

The local firewall 20 may be maintained in any conventional manner, such as by use of the Simple Network Management Protocol ("SNMP") on one or more computer systems 18 in the network 10. For example, SNMP may be used to poll, query, or otherwise control the local firewall 20.

In illustrative embodiments, the local firewall 20 must be configured prior to use. Configuration parameters may be derived from various sources. For example, the configuration memory 40 may have pre-loaded default

configuration parameters. In addition, the network administrator, network firewall 14, or the computer system 18 being protected may include a configuration program that automatically or manually forwards configuration data to the local firewall 20.

5   Figure 4 shows an illustrative process of configuring a local firewall 20 after it is connected to a computer system 18. The process begins at step 400, in which power is received by the local firewall 20 from the network 10. This power may be received via the power channel in the computer cable 24. Once converted to an appropriate level, the power is distributed to the elements in the

10   local firewall 20, thus permitting the local firewall 20 to operate.

Once energized, the configuration data is retrieved by the administration module 32 from both the configuration memory 40 (*i.e.*, the default configuration data) and the policy server 22 (steps 402 and 404). The local firewall 20 then is configured in accordance with the retrieved configuration data. At some later

15   time, it is determined if the configuration parameters are to be modified (step 408). This indication may originate from the prior noted configuration program(s) executing on either the network administrator's computer system or the local computer system 18 being protected. If modifications are required, then the local firewall 20 is reconfigured as specified by the reconfiguration data (step

20   410).

It should be noted that many other configuration processes can be used. Accordingly, the illustrative process of figure 4 is but one of many potential methods of configuring the local firewall 20. In fact, various steps in the noted process can be executed in an order that is different than that described.

25   In addition to configuring itself, the local firewall 20 may act as a proxy for its protected local computer system 18 when such computer system 18 initially joins the network 10. To that end, the computer system 18 registers with the router 16 or other relevant network device in a conventional manner using

the local firewall 20 as a proxy. Accordingly, the firewall may be considered to be transparent to the network 10.

In some embodiments, the local firewall 20 is configured to detect when someone has tampered with it. For example, to circumvent its security, someone may remove the local firewall 20 entirely, or replace the local firewall 20 with another local firewall 20 with other configuration data that permits access to the person tampering with it. Accordingly, in some embodiments, the local firewall 20 may include the tamper module 42 (noted above) to detect some of those events. In its simplest form, the tamper module 42 detects when an interruption of power to the local firewall 20 has occurred. The power interruption may be deemed to occur when power to a running local firewall 20 stops and then restarts. When the power interruption is temporary (*e.g.*, someone may be attempting to physically tamper with the local firewall 20), the tamper module 42 may forward a tamper message to the network administrator indicating that there was a temporary power loss. The network administrator may act appropriately to the message, such as by checking the identity of the local firewall 20. In other embodiments, an impedance detector may be used to detect a change in impedance in the line. If such impedance change is detected, the network administrator may be notified.

In other embodiments, the network administrator monitors power levels of all local firewalls 20 by means of SNMP. Among other things, this monitoring may be a polling operation, periodic transmission of "keep-alive" messages from the firewalls 20, use of intrusion sensors, or maintenance of a circuit with the local firewall 20. If any power interruption is detected, then the network administrator may take appropriate action. Power interruption may be deemed to occur when a local firewall 20 has been removed entirely, or when a local firewall 20 has been removed and subsequently replaced with another local

firewall 20. In fact, a power interruption may be deemed to occur when a local firewall 20 is removed and then re-coupled to the computer system 18.

In still other embodiments, the tamper module 42 or security module 34 may automatically forward a start-up message to the network administrator

5   upon receipt of power during its start-up phase. When the start-up message is received, the network administrator may take appropriate action. For example, if the start-up message is received during a valid start-up that is approved by the network administrator, no action may be taken. Receipt of a start-up message after a local firewall 20 has been operating for some time, however, may indicate

10   that such local firewall 20 is being tampered with, or is being replaced by another local firewall 20.

Some aspects of the invention may be implemented at least in part in any conventional computer programming language. For example, some embodiments may be implemented in a procedural programming language (*e.g.*,

15   "C") or an object oriented programming language (*e.g.*, "C++"). Alternative embodiments of the invention may be implemented as preprogrammed hardware elements (*e.g.*, application specific integrated circuits, FPGAs, and digital signal processors), or other related components.

Various components of the disclosed apparatus and method may be

20   implemented as a computer program product for use with a computer system. Such implementation may include a series of computer instructions fixed either on a tangible medium, such as a computer readable medium (*e.g.*, a diskette, CD-ROM, ROM, or fixed disk) or transmittable to a computer system, via a modem or other interface device, such as a communications adapter connected to a

25   network over a medium. The medium may be either a tangible medium (*e.g.*, optical or analog communications lines) or a medium implemented with wireless techniques (*e.g.*, microwave, infrared or other transmission techniques). The series of computer instructions embodies all or part of the functionality

previously described herein with respect to the system. Those skilled in the art should appreciate that such computer instructions can be written in a number of programming languages for use with many computer architectures or operating systems. Furthermore, such instructions may be stored in any memory device, such as semiconductor, magnetic, optical or other memory devices, and may be transmitted using any communications technology, such as optical, infrared, microwave, or other transmission technologies. It is expected that such a computer program product may be distributed as a removable medium with accompanying printed or electronic documentation (*e.g.*, shrink wrapped software), preloaded with a computer system (*e.g.*, on system ROM or fixed disk), or distributed from a server or electronic bulletin board over a network (*e.g.*, the Internet or World Wide Web), and/or as a data signal. Of course, some embodiments of the invention may be implemented as a combination of both software (*e.g.*, a computer program product) and hardware. Still other embodiments of the invention are implemented as entirely hardware, or entirely software (*e.g.*, a computer program product).

Although various illustrative embodiments of the invention are disclosed below, it should be apparent to those skilled in the art that various changes and modifications can be made that will achieve some of the advantages of the invention without departing from the true scope of the invention. These and other obvious modifications are intended to be covered by the claims that follow:

-14-

I claim:

1.   A firewall for use in a power integrated network having a plurality of computer systems, the firewall comprising:

5   an input module that receives data addressed to a given computer system in the power integrated network;

a security module operatively coupled with the input module, the security module analyzing the data received by the input module to determine if the data can be forwarded to the given computer system; and

10   a power module operatively coupled with the security module and input module, the power module receiving power from the power integrated network to energize the security module and the input module.

2.   The firewall as defined by claim 1 wherein the power integrated network

15   implements principles of Power Ethernet.

3.   The firewall as defined by claim 1 wherein the power module includes a power converter that converts power received from the power integrated network into a power level that can be used by the security module and the input

20   module.

4.   The firewall as defined by claim 1 further comprising an output module for forwarding the data to the given computer system.

25   5.   The firewall as defined by claim 1 further comprising a policy server interface operatively coupled with the security module, the policy server interface communicating policy data with a policy server.

6.   The firewall as defined by claim 1 wherein the power integrated network includes at least two computer systems coupled by a cable that transmits both data and power.

5   7.   A computer cable for communicating a first computer system with a second computer system in a power integrated network, the cable comprising:

a data channel for transmitting data between the first computer system and the second computer system;

a power channel for transmitting power between the first computer

10   system and the second computer system; and

a firewall coupled with the data channel and the power channel, the firewall being energized by power received from the power channel.

8.   The computer cable as defined by claim 7 wherein for bi-directional

15   communication, the data channel includes at least one data wire.

9.   The computer cable as defined by claim 7 wherein the power channel includes at least one power wire.

20   10.   The computer cable as defined by claim 7 further comprising a power converter that converts power received from the power channel into a power level that is capable of energizing the firewall.

11.   The computer cable as defined by claim 7 wherein the computer cable has

25   two ends, the computer cable further comprising:

a first coupler for coupling the first computer system with a first of the two ends of the computer cable; and

a second coupler for coupling the second computer system with a second of the two ends of the computer cable.

12.   The computer cable as defined by claim 7 further comprising a
5   containment layer circumscribing the data channel, the firewall, and the power channel.

13.   A firewall for use in a power integrated network, the firewall comprising:
        program code for receiving data addressed to a given computer system in
10   the power integrated network;
        program code for analyzing the received data to determine if the data can be forwarded to the given computer system;
        a processor for executing the program code for receiving and the program code for analyzing, the processor being energized by the power integrated
15   network.

14.   The firewall as defined by claim 13 further comprising a power module that receives power from the power integrated network to energize the processor.
20

15.   The firewall as defined by claim 14 wherein the power module includes a power converter for converting the power from the power integrated network to a power level that can be used to energize the processor.

25   16.   The firewall as defined by claim 13 wherein the power integrated network implements principles of Power Ethernet.

17. The firewall as defined by claim 13 further including a policy server interface for communicating with a policy server.

18. The firewall as defined by claim 13 wherein the power integrated network

5 includes at least two computer devices that are coupled by a cable that communicates both data and power.

19. A power integrated network coupled with a specified network, the power integrated network comprising:

10 a plurality of computer systems;

a network firewall coupled between the power integrated network and the specified network;

a local firewall coupled to one of the computer systems, the local firewall being powered by the power integrated network, the local firewall preventing

15 unauthorized access to the one computer system via the specified network, the local firewall preventing unauthorized access to the one computer system only.

20. The power integrated network as defined by claim 19 further comprising: a policy server coupled with the local firewall.

20

21. The power integrated network as defined by claim 19 wherein all of the computer systems in the power integrated network include a local firewall.

22. The power integrated network as defined by claim 19 wherein at least two

25 of the computers in the network are coupled by a cable that communicates both data and power.

23.   The power integrated network as defined by claim 19 wherein the power integrated network implements principles of Power Ethernet.

24.   The power integrated network as defined by claim 19 wherein the
5   specified network includes a public network.

25.   A method of securing a given computer system within a power integrated network, the method comprising:

receiving power from the power integrated network;
10   coupling a local firewall to the given computer system, the local firewall being configured to control access to the given computer system; and

using the received power from the power integrated network to energize the local firewall.

15   26.   The method as defined by claim 25 wherein the self–powering network includes a plurality of computer systems, at least one computer system in the network being coupled with the given computer system via a cable that transmits both data and power.

20   27.   The method as defined by claim 25 wherein the power integrated network includes an interface to a second network, the method further comprising:

coupling a network firewall to the interface to control access to the power integrated network.

25   28.   The method as defined by claim 25 wherein the power integrated network implements principles of Power Ethernet.

29.   The method as defined by claim 25 further comprising:

coupling the local firewall to a policy server to communicate policy data between the policy server and the local firewall.

ABSTRACT

A firewall that may be used in a power integrated network having a plurality of computer systems is powered by the power integrated network. To that end, the firewall includes an input module that receives data addressed to a given computer system in the power integrated network, a security module for determining if the data received at the input module can be forwarded tot he given computer system, and a power module to power both the input module and the security module. The power module receives its power from the power integrated network.

FIGURE 1

Firewall

20

30

24

26

28

FIGURE 2

To/from Computer Ethernet Card

To/from Router

to/from Router

20

38

INTERFACES

Power Module

36

Security Module 34

Administration Module 32

Config Data 40

Tamper Module 42

LOCAL FIREWALL

FIGURE 3

Begin

Receive
Power — 400

Retrieve configuration
data from policy — 402
server

Retrieve default — 404
data

configure — 406

modifications? — 408   NO

yes

Modify
as — 410
specified
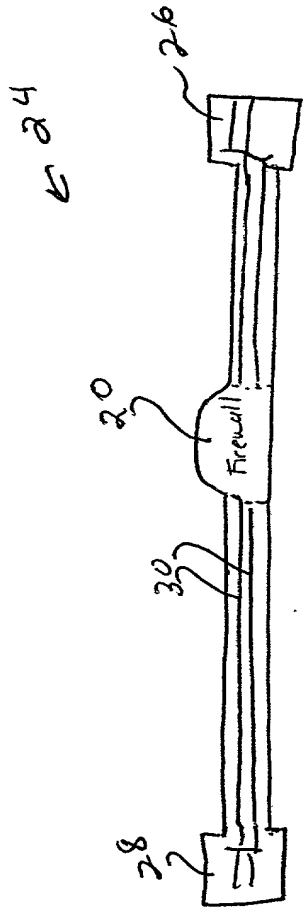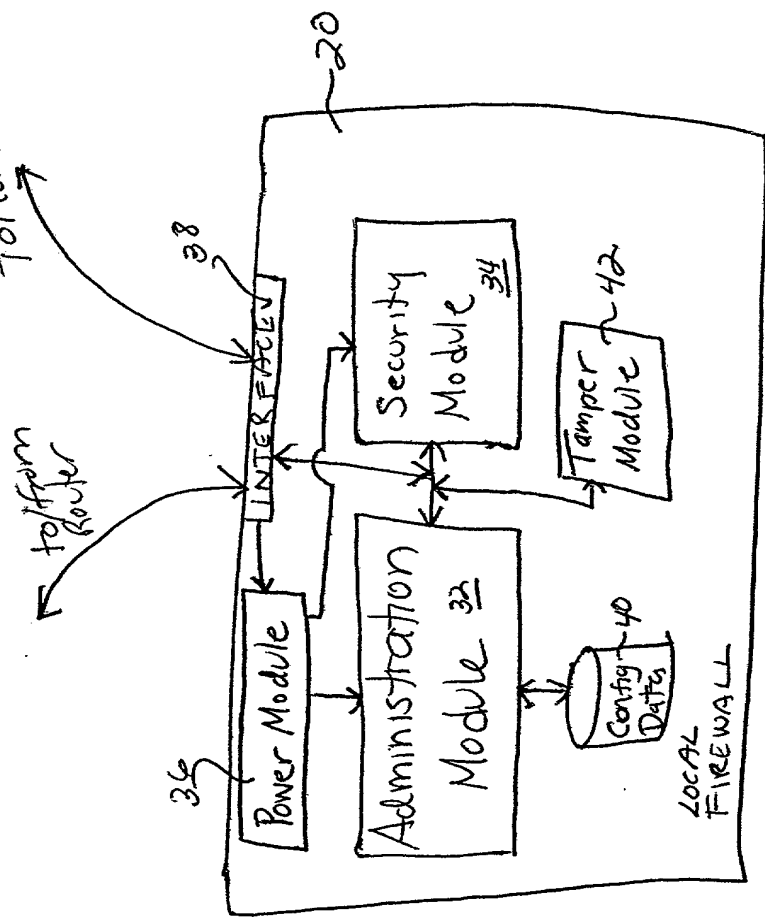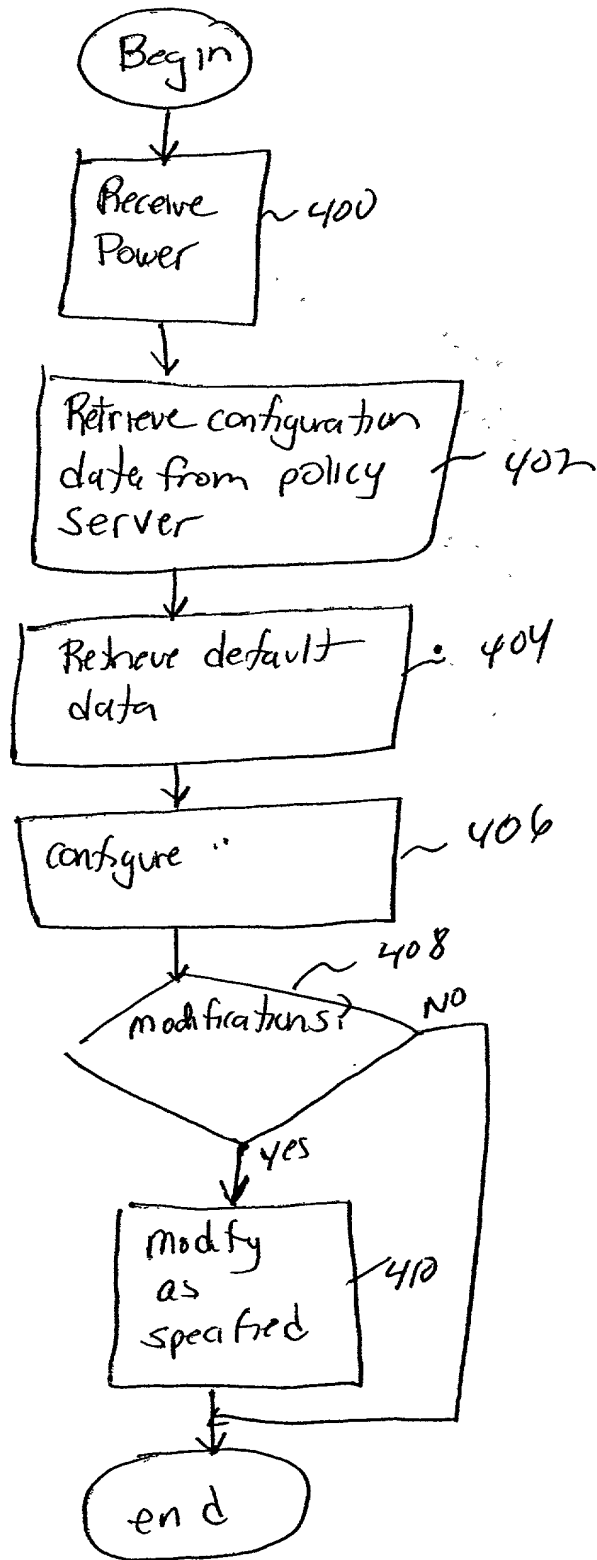
end

FIGURE 4

Docket No.
2204/A61

Declaration and Power of Attorney For Patent Application

English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

LOCAL FIREWALL APPARATUS AND METHOD

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on _____ as United States Application No. or PCT International

Application Number _____

and was amended on _____

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)   Priority Not Claimed

(Number)	(Country)	(Day/Month/Year Filed)	☐
(Number)	(Country)	(Day/Month/Year Filed)	☐
(Number)	(Country)	(Day/Month/Year Filed)	☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

_____   _____
(Application Serial No.)   (Filing Date)

_____   _____
(Application Serial No.)   (Filing Date)

_____   _____
(Application Serial No.)   (Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

_____   _____   _____
(Application Serial No.)   (Filing Date)   (Status)
                                                                        (patented, pending, abandoned)

_____   _____   _____
(Application Serial No.)   (Filing Date)   (Status)
                                                                        (patented, pending, abandoned)

_____   _____   _____
(Application Serial No.)   (Filing Date)   (Status)
                                                                        (patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Bruce D. Sunstein	Reg. No. 27,234	Jay Sandvos	Reg. No. 43,900
Robert M. Asher	Reg. No. 30,445	Sonia K. Guterman	Reg. No. 44,729
Timothy M. Murphy	Reg. No. 33,198	Keith J. Wood	Reg. No. 45,235
Steven G. Saunders	Reg. No. 36,265	Mary M. Steubing	Reg. No. 37,946
Harriet M. Strimpel	Reg. No. 37,008	Christopher J. Cianciolo	Reg. No. 42,417
Samuel J. Petuchowski	Reg. No. 37,910	Lindsay J. McGuinness	Reg. No. 38,549
Jeffrey T. Klayman	Reg. No. 39,250		
John J. Stickevers	Reg. No. 39,387		
Herbert A. Newborn	Reg. No. 42,031		
Elizabeth P. Morano	Reg. No. 42,904		
Jean M. Tibbetts	Reg. No. 43,193		

Send Correspondence to: Steven G. Saunders
Bromberg & Sunstein LLP
125 Summer Street
Boston, MA 02110

Direct Telephone Calls to: *(name and telephone number)*
Steven G. Saunders at (617) 443-9292

Full name of sole or first inventor **Stephen S. Jackson**	
Sole or first inventor's signature	Date
Residence **104 Antler Point Rd., Chapel Hill, NC 27516**	
Citizenship **U.S.A.**	
Post Office Address **Same as residence**	

Full name of second inventor, if any	
Second inventor's signature	Date
Residence	
Citizenship	
Post Office Address	

Form PTO-SB-01 (6-95) (Modified)　　　　　　　　Patent and Trademark Office-U.S. DEPARTMENT OF COMMERCE